Defense Security Service
Contractor SIPRNet Process
June 2013

Objectives

* Roles & Responsibilities
* Circuit Validation & Registration
* Required Equipment & Devices
* Certification & Accreditation
* Connection Approval Package
* SIPRNet Process Flow Chart

Roles and Responsibilities

Organizations	Responsibilities
DoD CIO	- Final approval authority for all connection requests in support of sponsor's mission
Defense Information Systems Agency (DISA)	- Responsible for management of Defense Information Systems Networks (DISN) circuits and oversight.
Government Sponsor	-Sponsor/owner of contractor connection - Provide funding for circuit and any other required services for contractor connection to SIPRNet (i.e. Computer Network Defense Service Provider (CNDSP), Host Based Security System (HBSS), email, Domain Name Service (DNS), SIPRNet Hardware Token and SIPRNet GIAP System Accounts).
DISA SIPRNet Service Management Office (SSMO)	- Review SIPRNet requests and initial topologies to determine whether the proposed DISN solution is appropriate. -Forwards the approved solution to DoD CIO for approval.
Defense Security Service (DSS)	- DAA for accrediting contractor information systems used to process classified information in industry – issues IATO, ATO and DATO.
DISA Certification and Accreditation Office/Classified Connection Approval Office (CAO)	- Process Connection Approval Packages (CAP) – issues Authority to Test/Connect IATT, IATC and ATC.

Circuit Validation

Government Contracting Authority (GCA)

* All Non-DoD Connections require a contract, MOU/A, and DoD Sponsor to validate mission need for partner access to DISN.

* Sponsors must adhere to responsibilities as stated in DoD CIO Sponsor Memorandum, dated 11 Jan 2012
  * Click here for Sponsor Memo

Circuit Validation

Sponsorship Letter (Validation request)

- Request must document all SIPRNet resources contractor will require (e.g. ports, protocols, services, websites)
  - Topology (complete & accurate)
    - Non-DoD Validation request: disa.meade.ns.mbx.siprnet-management-office@mail.mil
  - Approvals needed from: DISA SIPRNet Service Manager Office (SSMO), Sponsor's Service/Agency official, and DoD CIO
  - Full Validation is valid for three years or expiration of contract
  - Revalidation is required every three years or if change in sponsor, mission, requirements, contract or physical location (CAGE)
    - DoD CIO approval may be required. Example: Contractor relocating circuit to new facility or additional sponsor organization to existing circuit

CNDSP

CJCSI 6211.02D

For mission partner and defense contractor ISs, the sponsoring CC/S/A must ensure:

* A signed agreement (e.g., MOA) or contract defines the Computer Network Defense Service Provider (CNDSP) requirements, as specified in DODD O-8530.1, are included in the agreement
* CNDSP requirements are implemented prior to connection.

Circuit Order

Initiate SIPRNet Connection

* DISA Direct Online Entry (DDOE)
  * Sponsor creates account and submits Telecommunication Service Request (TSR)
  * Accurate POC information is critical to ordering process
  * Key personnel: Sponsor, Contractor FSO, ISSM and/or ISSO and COMSEC manager

Required Equipment & Devices

- All SIPRNet circuits require NSA Type 1 encryption (e.g. KIV 7M)
  - Sponsor must provide at both ends of SIPRNet circuit

- National Information Assurance Program (NIAP) approved Firewall (EAL-4) and Intrusion Detection System (IDS/IPS) (EAL-2) or Approved Products List (APL)

Circuit Registration

Circuit Sponsor must register connection information in the following systems/databases

* Network Information Center (SIPRNet Support Center)
* Ports, Protocols, & Services (PPSM)
* SIPRNet IT Registry

**Check DISA's Non-DoD Connection Process site for the above URLs/POCs for registration. **

Website: http://iase.disa.mil/connect/index.html

Certification & Accreditation

In accordance with DSS DISA MOA

* DSS is accrediting authority for NISP cleared contractor systems
  * Grants Authority to Operate (I/ATO) based on contract expiration date or three years whichever occurs first.

* DISA has management and oversight responsibilities of DISN
  * Grants Authority to Connect (I/ATC)
* Cleared contractor's systems must have both current ATO & ATC prior to processing on SIPRNet

Certification & Accreditation

System Security Plan and supporting documentation

* System Security Plan (SSP) and IS Profile
  * Utilize and configure systems to applicable DoD Secure Technical Implementation Guide (STIG)
  * Topology must include compliant Firewall/IDS and Routers
* Consent To Monitor (CTM) with sponsor signature
* Statement of Residual Risk (SRR) with contractor management signature (contractor personnel not GCA)
* Sponsor Validation/Re-Validation Letter
* DoD CIO Approval Letter

SIPRNet Requirements

- Command Cyber Readiness Inspections (CCRI)
  - Contractors subject to annual CCRI
- Utilization of DoD STIGs
- Compliance with USCYBERCOM directives
  - Including Host Based Security System (HBSS)
- SIPRNet Hardware Token
- Vulnerability Management System
- See DSS NISP SIPRNet Circuit Acquisition Process (NSCAP) for additional guidance
  - Formerly called DSS SIPRNet Contractor Approval Process (SCAP)

Connection Approval Package

Request for IATT, IATC/ATC

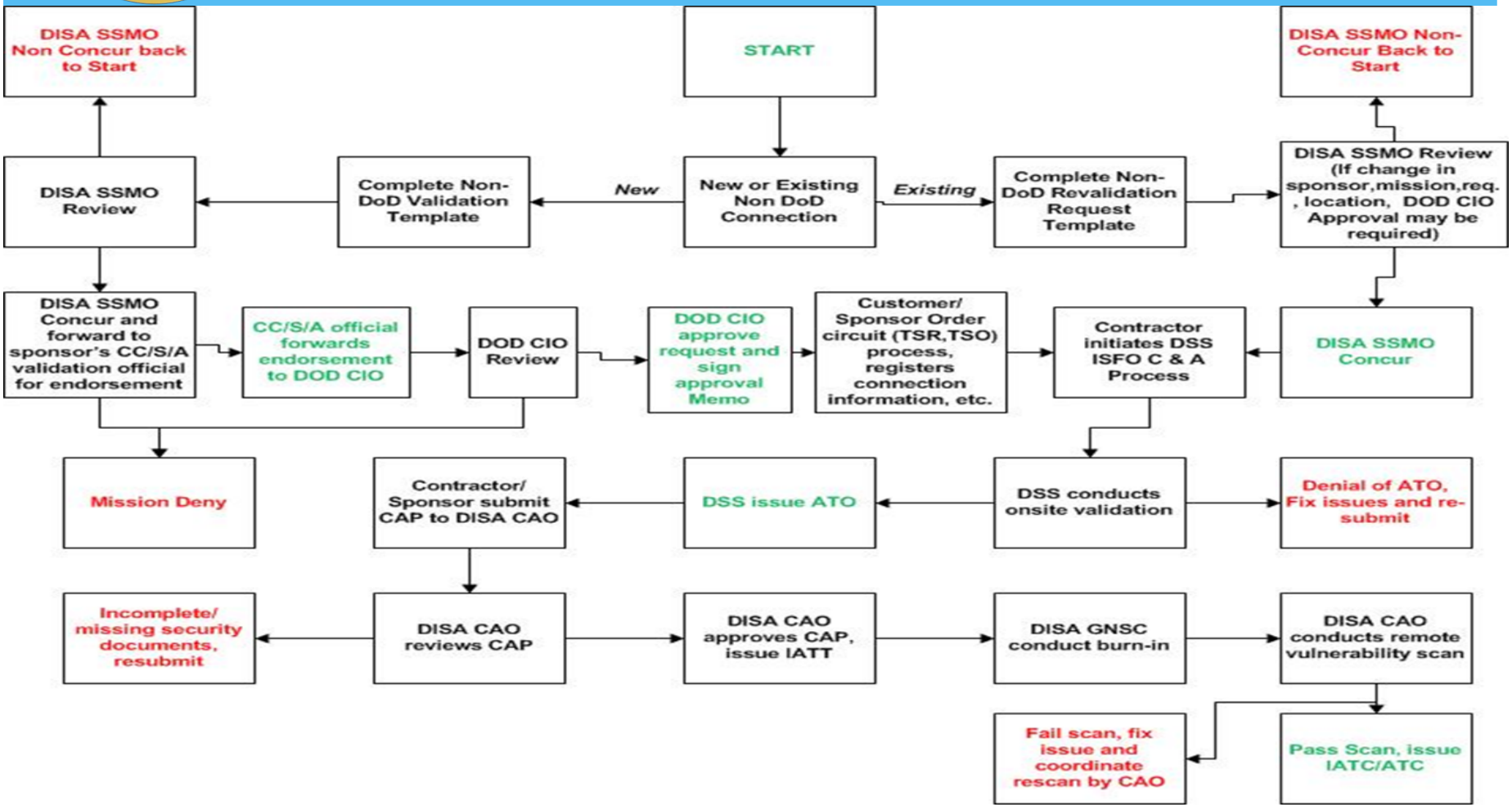
* Sponsor must register contractor system with SIPRNet GIG Interconnection Approval Process (GIAP)
* Sponsor and/or Contractor must upload the following documentation:
  * SSP, Network Topology, POA&M (if applicable), CTM, SRR, DSS ATO, Validation Memo, DoD CIO Approval Letter
* DISA CAO analyst will review for completeness
* New circuits will have 72 burn in implemented by DISA (IATT)
* DISA CAO will scan enclave prior to issuing IATC/ATC

Disclosure Authorization

- Contractors are NOT permitted unfiltered access to the SIPRNet (see CJCSI 6211.02D). The government sponsor determines requirements (validation letter/contract)

- Sponsor completes Disclosure Authorization Form with required ports/protocols and submits to DISA.
  - DISA will update contractor access list

SIPRNet Flow Chart


START
New or Existing Non DoD Connection
New
Existing
Complete Non-DoD Validation Template
Complete Non-DoD Revalidation Request Template
DISA SSMO Review
DISA SSMO Review (If change in sponsor,mission,req., location, DOD CIO Approval may be required)
DISA SSMO Non-Concur Back to Start
DISA SSMO Non Concur back to Start
DISA SSMO Concur and forward to sponsor's CC/S/A validation official for endorsement
CC/S/A official forwards endorsement to DOD CIO
DOD CIO Review
DOD CIO approve request and sign approval Memo
Customer/ Sponsor Order circuit (TSR,TSO) process, registers connection information, etc.
Contractor initiates DSS ISFO C & A Process
DISA SSMO Concur
Mission Deny
Contractor/ Sponsor submit CAP to DISA CAO
DSS issue ATO
DSS conducts onsite validation
Denial of ATO, Fix issues and re-submit
Incomplete/ missing security documents, resubmit
DISA CAO reviews CAP
DISA CAO approves CAP, issue IATT
DISA GNSC conduct burn-in
DISA CAO conducts remote vulnerability scan
Fail scan, fix issue and coordinate rescan by CAO
Pass Scan, issue IATC/ATC

Questions?

David Scott, CISSP

Sr, ISSP, Defense Security Service

David.scott@dss.mil